

WEBINAR

Mastering Workday: Ask an Expert Series

Session: Innovations in Workday Human Capital Management Tenant Security Governance & Solutions



WELCOME

Today's Expert



Joe Kelly

Senior Manager, Consulting
Armanino

Session

Innovations in Workday Human Capital Management Tenant Security Governance & Solutions

- **Importance of Security Controls and Governance**
Learn how Armanino helps clients implement this model in Workday HCM.
- **Innovative Security Group Solutions**
Explore three solutions and their applications for effective use.

Engagement Encouraged!



- **Interactive Q&A Sessions:**
Get your specific Workday questions answered live by our experts, ensuring you leave with practical solutions tailored to your needs.
- **Expert Insights & Tips:**
Gain exclusive access to professionals who will share valuable insights, tips, and best practices to enhance your Workday experience.
- **Real-World Case Studies:**
Learn from real-world use cases that showcase how other organizations are successfully leveraging Workday to solve common challenges and drive business success.



Security Governance Tips

- Limit Ownership System Security



Access Requires a Business Reason

- Audit Group Membership



Add/Remove users regularly

- Always Test Security Modifications



Admin Proxy Tests & Security Reports

- Leverage Existing Groups



Paring down > Building up

Custom Security Group Solutions

ABSTRACT

Narrow down self-service actions by intersecting common delivered groups with custom created membership groups

Steps

- Create Source Group to dynamically determine membership
 - *Ex: Location Membership, Management Level*
- Create Intersection Group
 - *Intersect Location Membership with EE as Self*

Use Cases

- Phased module rollouts by country/location
 - *Ex: Benefits is live in the USA, but not India until 2025*
- Different allowed actions by types of workers
 - *Ex: Hourly workers can submit time, but salaried workers cannot*
- Narrowing down compensation view access for role-based groups
 - *Ex: Managers can view compensation in their organization only if they are "Director" and above*

ABSTRACT

Narrow down user actions by intersecting delivered groups such as All Users or EE as Self with groups using a custom security rule to dynamically determine membership.

Steps

- Create Rule Based Security Group
- Create Security Rule
 - *Worker object (in most cases)*
 - *Select a logical value to reduce access*
- Select a baseline group

Use Cases

- Necessary Authentication Policy Adjustments
 - *Ex: Workers on Leave can bypass SSO because they cannot authenticate OR Restrict access for all Unpaid Leaves*
- Restrict/Allow access based on Checked In Status (if using Workday Time)
- Any restrictions needed based on *multiple* conditions

ABSTRACT

Build groups on top of each other using custom data points created to isolate users to allowable segmented security values. Useful for subjective or selective access to specific instances

Steps

- Create a custom value (Org or Object) to selectively assign to workers
- Create an initial security group to limit users, intersect with applicable delivered group (i.e., EE as Self)
- Create Segmented Group to restrict access to item
 - *Ex: Learning Topics, Doc Categories, Talent Statements*

Use Cases

- Sensitive Learning Topics & Courses
- Specific Document Category Access (View/Modify)
- Negotiated Compensation Plans Required Limited Visibility to Assignments
- Questionnaires of a Delicate Nature (Exit Surveys)
- Personal Talent Statements

****Only Use if no tenanted data exists to narrow down users****

Thank you for
attending

Additional Questions?

Reach out to us at

Experts@armaninio.com

